EC-2000-007
IV-D-057

Docket #: EC-2000-007

February 20, 2002

United States Environmental Protection Agency
Enforcement and Compliance Docket and Information Center
Mail Code 2201A
Attn: Docket Number EC-2000-007
1200 Pennsylvania Avenue NW
Washington DC 20460

RE: Proposed Cross Media Electronic Reporting and Record-keeping Rule

To Whom it May Concern:

Ohio EPA appreciates the effort that U.S. EPA has made to include the states in crafting the Cross Media Electronic Reporting and Record-keeping Rule (CROMERRR). We agree with the need to ensure security and integrity of electronically exchanged data. However, we have serious concerns about the rule in its current form. I would like to emphasize several key concerns to Ohio.

One of the goals of CROMERRR, as stated in the overview, is overall cost reductions to regulated entities and state agencies, but that goal does not appear to be achieved. The State of Ohio has been accepting data electronically in most of its media programs for several years. Millions of dollars have been invested to develop systems that allow the regulated community the flexibility of electronic reporting while also streamlining the state's ability to submit data to U.S. EPA.

We estimate that to implement CROMERRR for the electronic reporting component alone would cost approximately $3.75 million dollars. We estimated our current number of electronic filers at 6,220. Using the State of Washington scenario of a High Assurance digital certificate stored on a SmartCard with Reader at a cost of $131.00 annually, the cost to implement the digital certificate requirement of CROMERRR could cost the regulated community or taxpayer as much as $814,820 annually. Electronic record-keeping costs for both our regulated entities and this agency are not included with this response.

CROMERRR requirements call for increased system security beyond what Ohio EPA now has in place and we agree that enhanced security measures are needed. However, the prescriptive security and tracking requirements proposed for electronic exchange of data far exceed those for paper submissions and go well beyond the intent of this rule. This is a concern since electronic commerce is rapidly replacing paper as the standard. U.S. EPA has standards for receipt of data via paper, but does not dictate a process to be followed.

CROMERRR also should focus on establishing standards for electronic data exchange; rather than dictating the process.

CROMERRR claims technological neutrality; however, only a very few current technologies would meet CROMERRR's requirements and those technologies are largely untested. The state of Ohio has taken the approach that security requirements for electronic signatures and records used by Ohio state agencies fall within one of four security levels ranging from the minimum security necessary to the most stringent necessary. Ohio state agencies determine the security level for a given electronic transaction by conducting a risk analysis that identifies the potential impact of a security breach and the likelihood that someone would attempt to breach security for the given electronic transaction.

Once a security level is determined for an electronic transaction, then there are minimum standards that must be met. This approach avoids implementing requirements that are too stringent for relatively low-risk transactions and assures that stronger requirements exist for very high-risk transactions. The regulatory structure for Ohio state agencies is set forth in rule 123:3-1-01 of the Ohio Administrative Code (attached).

Moreover, due to the current budget situation and economic conditions, Ohio would be unable to implement all of the prescriptive requirements of CROMERRR within the one to two years post promulgation time frame. CROMERRR does not currently contain a provision for grand-fathering of existing electronic reporting systems. Without a realistic grandfather provision, Ohio would be forced to discontinue use of its current electronic reporting systems and revert to reporting via magnetic media or a paper system. Reverting to a paper system would come at the unnecessary and unreasonable cost of abandoning our investment in our existing systems while also undermining pollution prevention, burden reduction, and electronic reporting goals.

Conversely, CROMERRR has been proposed as a voluntary rule, in that state agencies may abide by the rule or submit data on paper or via magnetic media. However, for states such as Ohio, which already accept and submit data electronically and are bound by agreement with US EPA to continue, the rule is clearly mandatory. We request that all currently operating electronic systems supporting electronic exchange of data in place prior to promulgation of CROMERRR be grand-fathered for a period of time negotiated on a case-by-case basis. For Ohio EPA, given current funding, we would need a minimum of 5

The timing issue is complicated for Ohio because the State is in the midst of establishing its own requirements for electronic exchange of data. A pilot project involving the use of Public Key Infrastructure (PKI) is in the planning stages as well as design of a state web portal for information exchange. The State requirements are not yet known, but will need to be addressed when Ohio EPA implements CROMERRR. This state project further demonstrates the need for a flexible grand-fathering provision.

Detailed comments on specific sections of the proposed rule are attached. As required by

the August 31, 2001 announcement in the Federal Register, three copies of this letter and comments are attached.

Please direct any questions to Adele Vogelgesang, Office of Data and Systems, at (614) 728-1747 or email: adele.vogelgesang@epa.state.oh.us.

Sincerely,

Christopher Jones
Director

JA/AV/av

Cross Media Electronic Reporting and Record-Keeping Rule
Ohio EPA Public Comment Response
Docket #: EC-2000-007
February 13, 2002

General Comments:

Fulfillment of Goals

The goals of CROMERRR are to:

1. Reduce cost and burden of data transfer and maintenance for all parties
2. Improve data quality and speed and convenience of access to data.
3. Maintain or improve level of accountability and responsibility for electronic

US EPA REQUESTED COMMENT ON HOW WELL THE CROMERRR PROVISIONS AND THE CENTRAL DATA EXCHANGE (CDX) WILL FULFILL THESE GOALS.

Response:

For states with operating Electronic Environmental Information Exchange systems, US EPA must work closely with the states and provide support and technical expertise to help prepare states' ability to participate in the National Environmental Information Exchange Network. The recent Grant program established to further Network development will assist with this effort.

However, in goal #1 above, the cost of upgrading already existing electronic reporting systems so that they meet CROMERRR requirements is a significant cost to delegated programs and regulated industry. The State of Ohio has been accepting data electronically in most of the media programs for several years. Millions of dollars have been invested to develop systems that allow the regulated community the flexibility of electronic reporting while also streamlining the state's ability to submit data to U.S. EPA. CROMERRR requirements call for increased system security beyond what Ohio EPA now has in place and we agree that enhanced security measures are needed.

However, due to the current budget situation and economic conditions, Ohio would be unable to implement all of the prescriptive requirements of CROMERRR within the proposed time frame. A realistic grandfather provision is needed and without it Ohio would be forced to discontinue use of its current electronic reporting systems and revert to reporting via magnetic media or a manual paper system. Reverting to a paper system would come at the unnecessary and unreasonable cost of abandoning our investment in our existing systems, while also undermining pollution prevention, burden reduction, and electronic reporting goals.

Please note the Reporting chart below showing some of the data flows largely supported by currently operating electronic enterprise-wide systems:

Type Data	Amount of Data received	Frequency of receipt	ER system initiated with Data Entry Module (DEM)	Amount of regulatory data sent to US EPA	Frequency of sending to US EPA	Amount of primacy-related data sent to US EPA
*HW Annual Report	1200 reports with some reports up to 30,000 rows of data. Approx 360 received electronically (via DRUMS DEM) with 840 received on paper.	Annually	2001 first use of DRUMS DEM, but for years prior used ASCII mailed on diskette.	1200 reports (only data of odd-numbered years is reported). Ohio EPA data enters the 840 reports into its EDM-related DRUMS system.	Biennially	NA
Drinking and Ground Waters	5700 MOR's and SSR's via DRINKware DEM.	Monthly	Year 2000; Submitted via MSIS (legacy system) prior to DRINKware DEM	approx. 300,000 lines of info representing non-compliance	Quarterly	approx. 400,000 lines of info representing inventory of WTP/water systems

Air-related	**1. 200 Permits to Install (PTI's) 2. 780 Title V Fee Emission reports received via STARship DEM 3. 780 Emissions Inventory summaries received via STARship DEM 4. 500 facilities report risk manage-ment data 5. 11,500 PTO applications w/780 Received electronical-ly (via STARship DEM) as required by Title V. Approx 5% of remaining 10, 720 send elec with remaining on paper. 6. Approx. 2400 anticipated Non-Title V Fee Emission Reports	1. Monthly 2. Annually 3. Annually 4. 5-year cycle (300 facilities report via magnetic media) 5. 5-year cycle 6. Biennially beginning 2004	1. None 2. 1995 3. 1995 4. Via magnetic media 5. 1995 6. Planned for 2004 via STARship 2 DEM	1. 150/mo. 2. 780 issued PTO's on a 5-year renewal cycle 3. 780 facility EIS reports 4. None 5. 100 PTO's/mo. 6. Approx. 2400	1. As issued 2. None 3. Annually 4. None 5. As issued 6. Biennially beginning circa 2004	

Surface Water/DMR	186,000 on paper and 194,000 electronically (via SWIMware DEM)	Monthly	1999 (from 1995 on accepted reports electronically, but signed paper copy required for signatory requirements.	43,750 PCS measurement transactions	Monthly	

*** Ohio is #1 nationally in HW receipts.**
**** 200 PTI's in Air program sent on paper, but setting up for electronic transfer is in-process.**
***** Representative Sample of Program Data Flows/does not represent all data flows of agency**
DEM = Data Entry Module
DMR = Discharge Monitoring Report
DRUMS = Data Retrieval and Utility Management System
(based on the agency Enterprise Data Model)
EDM = Enterprise Data Model
EIS = Emission Inventory Summary
ER = Electronic Reporting
GW = Ground Water
HW = Hazardous Waste
MOR = Monthly Operating Report
MSIS = Model State Information System (Drinking and Ground Waters system)
PCS = Permit Compliance System
PTI = Permit to Install
PTO = Permit to Operate
SSR = Sample Submission Report
TRI = Toxic Release Inventory
WTP = Water Treatment Plant

Note: US EPA wants electronic submission of compliance and inspection data from the Air program by 4/2002 on a quarterly basis. Interim fix of a Visual Foxpro system, but plan to incorporate into the STARS 2 EDM-related system.

The timing issue is complicated for Ohio because the State is in the midst of establishing its own requirements for electronic exchange of data. A pilot project involving the use of Public Key Infrastructure (PKI) is in the planning stages as well as design of a state web portal for information exchange. The State requirements are not yet known, but will need to be addressed when Ohio EPA implements CROMERRR. This state project further demonstrates the need for a flexible grand-fathering provision.
supporting electronic exchange of data in place prior to promulgation of CROMERRR be grand-fathered for a period of time negotiated on a case-by-case basis.

The prescriptive security and tracking requirements proposed for electronic exchange of data far exceed those for paper submissions. This is a concern since electronic commerce is rapidly replacing paper as the standard. U.S. EPA has standards for receipt of data via paper but does not dictate a process to be followed. CROMERRR also should focus on establishing standards for electronic exchange of data rather than dictating the process. CROMERRR claims technological neutrality; however, only a very few current technologies would meet

CROMERRR'

The Effect on Smaller Regulated Entities

US EPA REQUESTED COMMENT ON WHETHER THIS RULE WOULD MAKE ELECTRONIC REPORTING (ER) MORE ATTRACTIVE TO SMALLER REGULATED ENTITIES.

Response:

If the ER interface is Web-based and easy to use, it would be attractive to all companies that have Internet access. However, for electronic record-keeping, Subpart C states that the scope of CROMERRR includes any data the regulated community is keeping in accordance with the regulations and which is maintained electronically. If businesses must adhere to stringent security/audit protocols that are not currently in use or require them to expend money for software or hire personnel with the sufficient experience, Electronic reporting and record-keeping will not be practical or attractive.

Risk Analysis for Data:

There are no provisions for differing levels of assurance in CROMERRR. In the private and public sectors there appears to be a widespread, common approach that security technologies and procedures depend in part on the risks associated with the records that are to be protected balanced with the cost of protecting the records. Even within public key infrastructures, there are often varying levels of protection depending on the security requirements of the record being protected (e.g., Federal Bridge Certification Authority's X.509 certificate policy and Canada PKI certificate policies). Ohio's *Uniform Electronic Transactions Act* or UETA (Ohio Revised Code 1306.01 - 1306.23) recognizes that what is "secure" depends on the context by permitting parties to reach agreement as to what will constitute an electronic signature. The only qualification on this freedom to contract is that it be "commercially reasonable."

The state of Ohio has taken the approach that security requirements for electronic signatures and records used by Ohio state agencies fall within one of four security levels ranging from the minimum security necessary to the most stringent necessary. Ohio state agencies determine the security level for a given electronic transaction by conducting a risk analysis that identifies the potential impact of a security breach and the likelihood that someone would attempt to breach security for the given electronic transaction. Once a security level is determined for an electronic transaction, then there are minimum standards that must be met. This approach avoids implementing requirements that are too stringent for relatively low-risk transactions and assures that stronger requirements exist for very high-risk transactions. The regulatory structure for Ohio state agencies is set forth in rule 123:3-1-01 of the Ohio Administrative Code (attached).

CROMERRR does not set out the requirements in common electronic signature terms of authentication, authorization, integrity and nonrepudiation. Furthermore, CROMERRR mixes the concepts of authentication and authorization.

Security for a given record will never be 100%. Some of the requirements set forth in

There seems to be an element of reasonableness missing from CROMERRR. Some of the things that CROMERRR would require that a system prove cannot be proved with 100 percent certainty. For example, CROMERRR would require proof "[i]n the case of documents requiring the signature of an individual, that the document was actually submitted by the authorized signature holder and not some other person." (Section 3.2000 (b)(3)). Because the authorized individual could intentionally or negligently give out the access code or device, a state agency or business could never prove that only the authorized individual did the signing.

COMMENTS SOUGHT ON WHETHER SPECIFIC CROSS-REFERENCES TO ANNOUNCEMENTS AND INSTRUCTIONS TO THE EXTENT THESE ARE CODIFIED SHOULD BE PROVIDED TO SHOW PROGRAM-SPECIFIC REGULATIONS FOR WHICH ER OR ELECTRONIC RECORD-KEEPING HAS BEEN IMPLEMENTED AND INVITES SUGGESTIONS ON HELPFUL CROSS-REFERENCING SCHEMES.

Response:

Yes, a cross-referencing scheme should be used. No recommendations at this time.

US EPA SEEKS COMMENTS ON WHETHER OR NOT 1-6 BELOW SHOULD BE INCLUDED IN CROMERRR AND WHETHER EXISTING PAPER DOCUMENTS SHOULD BE CONVERTED TO ELECTRONIC DOCS AND COMMENTS ON THE STRENGTHS AND WEAKNESSES OF EXISTING TECHNOLOGIES AVAILABLE FOR THIS PURPOSE.

Additional Provisions under Consideration

US EPA is considering whether to include additional provisions in CROMERRR to include:

1. Written policies to limit system access to authorized personnel; use of authority checks to ensure only authorized personnel can use system, sign a document electronically, access computer system input or output device, alter a record or perform the operation at hand.
2. Written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures.
3. Use of device checks to determine validity of the source of data input or operational instruction.
4. Use of document encryption and use of digital signature standards.
5. Routine and documented validation of systems.
6. Written policies governing education and training of personnel.

Response:

Ohio EPA agrees that #2 and #4 might be appropriate for high risk data as determined by a risk analysis. It is acceptable to impose #1, #5, and #6 on electronic receivers. But there will be reluctance to conduct ER if resource-intensive high-tech requirements are imposed on the sender. And the impact of Subpart C also is a factor in determining what standards to use on which type of electronically stored information.

US EPA ALSO SEEKS COMMENT ON WHETHER EXISTING PAPER DOCUMENTS SHOULD BE CONVERTED TO ELECTRONIC DOCUMENTS.

Response:
This should be left to the discretion of the facility (regulated entity) or delegated program as long as they can readily produce a copy of the document for inspection purposes.

US EPA SEEKS COMMENT ON WHETHER THE INCORPORATION OF THE CDX "BUILDING BLOCKS" WILL ENSURE THE VALIDITY OF ELECTRONIC DOCUMENT RECEIVING SYSTEMS.

Response:

The required 'key building blocks" of CDX include:

-
- a process for registering users and managing their access to the CDX,
- a characteristic systems architecture,
- electronic data interchange (EDI) standards, and
- a characteristic environment in which electronic reporting transactions will be conducted.

Does EPA intend to mandate that the same technologies (specifically PKI and EDI) be used by states that administer electronic reporting systems? If not, this should be clearly stated that this is not the intent so "certifying" parties do not interpret it as such.

Storage Media Issues

EPA's discussion gives an example that, "a CD-ROM version of a record originally stored on electromagnetic tape would not satisfy federal record keeping requirements unless the method for transferring the record from one medium to the other employed error-checking software to ensure that the data was completely and faithfully transcribed.".

Response:
CROMERRR does not make clear to what degree "error checking" must take place to satisfy the

While error-checking is typically conducted during all data conversion processes and is common practice, this requirement seems unnecessary. Although good business practice, no such requirements are in place for hard copy submissions that are transferred to an electronic format either through scanning or key-punching.

ER DOCUMENT RECEIVING SYSTEMS MUST EMPLOY ERROR-CHECKING SOFTWARE TO ENSURE THE DATA IS COMPLETELY AND FAITHFULLY TRANSCRIBED. IS THIS CRITERION SUFFICIENT TO ENSURE AN ER IS AUTHENTIC/MAINTAINS ITS INTEGRITY THROUGHOUT ITS RECORD RETENTION PERIOD?

Response:

Subpart C states that the scope of CROMERRR includes any data the regulated community is keeping in accordance with the regulations and which is maintained electronically. If businesses must adhere to stringent security/audit protocols that are not currently in use or require them to expend money for software or hire personnel with the sufficient experience, Electronic record-keeping will not be practical or attractive.

Separate Criteria for Non-Certified or Certified on Paper

US EPA SEEKS COMMENT ON WHETHER IT SHOULD DEVELOP A SEPARATE SET OF CRITERIA FOR RECEIVING SYSTEMS WHICH WOULD NOT ACCEPT ELECTRONIC SIGNATURES OR WHERE

Response:

If a document does not require a signature, this "Validity of Data" should not be required of those documents. A risk analysis as outlined in Ohio Administrative Code (OAC) 123-3-1-01 should determine what level of security is required. Separate sets of criteria should be established based on the security level appropriate.

HOW WILL SELF-MONITORING AND SELF-REPORTING SYSTEMS BE AFFECTED BY CROMERRR IN COMPARISON TO ITS PAPER REPORTING COUNTERPART?

Response:

The CROMERRR criteria seem to be designed for submission of environmental compliance data. Our existing system allows the electronic submissions of ***permit applications***. In cases where this is a new permit, we have not established a "regulatory" relationship with these facilities and therefore, would not have a valid individual electronic signature for them. We do allow electronic submissions using a "default" PIN, but require a signed hard copy applications be sent as well. Ohio is assuming that the CROMERRR standards would not apply to this portion of our system for processing permit applications, since a follow-up hard copy is required.

Specific Comments:

p. 46189, Subpart A, Section 3.3: Definitions

Electronic document means a document that is submitted to an agency or third-party as an electronic record, and communicated via a telecommunications network. For purposes of this part, electronic document excludes documents submitted on such magnetic media as diskettes, compact disks or tapes; it also excludes facsimiles.

Electronic record means any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.

Response: What is the difference between an electronic document and an electronic record?

Electronic document receiving system means any set of apparatus, procedures, software, records or documentation used to receive documents communicated to it via a telecommunications network.

Response: Does this include interactive voice response systems (if needed)?

p. 46190, Subpart B, Section 3.20: Public Notice of Changes

without requiring a new rule. However, it is also recognized that some changes (termed **major**) may then require changes by the regulated community in software or hardware e.g. Changes in file formats CDX will accept, or changes in electronic signature technology. **Minor** changes might include changes in screen layout, sequencing of user prompts, etc **Transparent** changes might include a change to the archiving process and an **Emergency** change might involve the need to upgrade the firewall. See p. 46169, section IV.A.

CROMERRR proposes to:

PUBLIC NOTICE THE MAJOR CHANGE 1 YEAR IN ADVANCE OF PLANNED IMPLEMENTATION. MINOR CHANGES NOTICE 60 DAYS IN ADVANCE. TRANSPARENT AND EMERGENCY CHANGES WOULD BE NOTICED ON A CASE-BY-CASE BASIS. COMMENT SOUGHT ON THESE PROPOSED TIME FRAMES, AND DESCRIPTION OF TYPES OF CHANGES.

Response:
Ohio EPA recommends a minimum 1-year notice should be made for **major** changes, with a public notice. Because US EPA usually consults with the states on major changes, the states will probably be aware of the prospective major changes before the 1 year time period begins. However, Ohio operates on a biennium budget. If a major change requires states to expend a significant amount of money, more than 1-year's notice is necessary.

p. 46190, Subpart C, section 3.100 Electronic Record keeping under EPA Programs

Response:
Requirements are overly burdensome and extremely resource intensive to implement and maintain. The amount of "metadata" (i.e. data about data) associated with electronic signature and submissions will often be more than the environmental data itself. Again, EPA states that, "These criteria are intended to facilitate the ability of plaintiffs and prosecutors to successfully defend against attempts by regulated entities to repudiate their own electronic records and documents." CROMERRR's main purpose should not be for the "ease" of criminal prosecution, but the ease of data submission!

Section 3.100

Ref **(a) (1)** on maintaining records in a "form" that may not be altered without detection

Response: By using the word "form," it appears that PKI is required. There are systematic approaches to electronic signatures such as access controls with audit-logging that meet this requirement without relying on the form of the document to detect alterations.

Ref **(a) (5)** "detached, copied, or otherwise compromised."

Response: "Disassociated" would be a better term to use instead of "detached."

Ref **(a) (8)**: Ensure that electronic records and electronic documents are searchable and retrievable for reference and secondary uses, including inspections, audits, legal proceedings, third party disclosures, as required by applicable regulations, for the entirety of the required period of record retention;

Response: Requirement (a)(8) is functionally necessary for ease of access. It is not necessary to show the validity of an electronic record.

Ref **(a) (9)**:

Response: The long-term preservation of digitally signed electronic documents could be problematic. Currently, there are no mechanisms in place that can ensure the long-term preservation and accuracy of digital signatures.

US EPA SEEKS COMMENTS ON WHICH LISTED OPTIONS FOR ARCHIVING SHOULD BE INCLUDED AS REQUIREMENTS FOR ELECTRONICALLY-MAINTAINED RECORDS.

Response: The possibility of reformatting in order to ensure long-term preservation; including reformatting into an eye-readable format such as paper or microfilm should be addressed.

p. 46190, Subpart C, 3.100

Requirements for Electronic Records

Response:

The scope of CROMERRR includes any data the regulated community is keeping in accordance with the regulations and which is maintained electronically. Examples of electronic records currently being kept by some RCRA-regulated facilities include:

1. Waste analysis records (e.g., waste profiles, analytical laboratory reports)
2. Waste inventory records (e.g, bar code systems for tracking wastes managed at facility)
3. Customer Information (e.g., type of industry, facility contacts, billing invoices)
4. Personnel training records (e.g., dates of required annual training and list of attendees)
5. Inspection records (e.g., inspection of regulated units & required emergency equipment)
6. Ground water monitoring data
7. Waste shipment records (e.g., manifests, LDR notifications, tolling agreements)

Several of these records are accessed by the facility to compile reports that the agency requires,

such as the annual Hazardous Waste Report or the Supplementary Report for Ground Water Monitoring. Others are kept on-site only, but may be viewed by agency inspectors when they visit the facility.

We are concerned about the impact that CROMERRR may have on any required data that happens to be kept electronically at the facility. The security and audit trail requirements of Subpart C could prohibit electronic record-keeping by facilities who do not have sophisticated systems, especially those which are small businesses. In addition, the facility staff and Ohio EPA inspectors may not be qualified to determine whether the methods currently used would be deemed "acceptable" without guidelines easily understood by non-Information Technology (IT) professionals.

A matrix should be developed for ranking purposes. There is a need to distinguish between electronically stored data required to be certified and submitted to government versus that which is only maintained on-site. The vulnerability (risk of data compromise) and impact (cost of compromise of data) need to be balanced against the type of information and the requirements for it. Please refer to Ohio Administrative Code (OAC) 123:3-1-01 Use of Electronic Signatures and Records attached.

Another resource recommended by the Ohio Historical Society/State Archivist Office for records management is DoD 5015.2 and the National Archives and Records Administration (NARA). This department will be responding to CROMERRR under separate cover letter.

p. 46191, Subpart D, section 3.1000
Electronic Reporting and Record-keeping Under EPA-Approved State Programs
How are authorized State, tribal or local environmental programs modified to allow electronic reporting?

Response: Ref paragraphs (a) and (b) which would require a significant change in state systems. It is not clear that the U.S. EPA has identified the impact on current electronic reporting systems which will have to be modified or revised under this paragraph. Ohio EPA estimates that to implement CROMERRR for the electronic reporting component alone would cost approximately $3.75 million dollars. We estimated our current number of electronic filers at 6,220. Using the State of Washington scenario of a High Assurance digital certificate stored on a SmartCard with Reader at a cost of $131.00 annually, the cost to implement the digital certificate requirement of CROMERRR could cost the regulated community or taxpayer as much as $814,820 annually.

Ohio EPA's Division of Hazardous and Waste Management has an annual requirement for the Hazardous Waste Report versus the federal frequency of biennial. If CROMERRR becomes a final rule and if our program is not approved by US EPA before December 2002 then we will not be able to use the electronic reporting system already in place. Therefore US EPA should consider grand-fathering ER programs that are already in place in authorized states to give the states time to modify their systems and to give US EPA sufficient time to evaluate the program.

p. 46191, Subpart D, section 3.2000
Electronic Reporting and Record keeping Under EPA-Approved State Programs
What are the criteria for acceptable electronic document receiving systems?

Ref **(a) (1,2, and 7)** on "strong and effective protections"

Response: The term "strong and effective protections" needs to be defined.

Ref **(b) (1-3)**

Response: This section is missing a reasonableness standard. Requirement (b)(1) and (b)(2) cannot be proved with 100% certainty. Requirement (b)(3) is very difficult to prove. Short of biometrics or implanted chips, a system has no way of being able to collect data that proves that the signature holder has not given out the signature mechanism (token, code, password, etc.) to some other person.

Ref **(c)**

Electronic signature validation system will:

1.Use a registration process.

2.Include a signature certification process.

3. Include safeguards to prevent excise, modification or appropriation of an affixed electronic signature.
4. Includes safeguards to prevent use of an electronic signature by anyone other than the individual.
5. Ensures any modification of a document after signature is detectable (signature is bound to the contents of the report).

US EPA SEEKS COMMENTS ON WHETHER 1-5 ARE APPROPRIATE AND WHETHER 1-5 ENSURES THE SAME OR BETTER EVIDENTIARY VALUE AS HANDWRITTEN SIGNATURES ON PAPER DOCS.

Response:

EPA has put in place painstaking requirements that prevent repudiation and alteration of electronic data through transmission and during storage, yet there is a requirement that the signature be "bound" to the electronic submission (#5 above). This seems to be redundant and unnecessarily burdensome.

Ref **(c) (5)**

Response: Ensuring the impossibility of modification is itself impossible. Security using cryptography may be broken given enough time and resources.

p. 46191, subpart D, section 3.2000
Electronic Reporting and Record-keeping Under EPA-Approved State Programs

State Electronic Report Receiving Systems must satisfy certain criteria to be allowed to receive ER as a delegated State. The criteria are set in order to ensure that any electronic document used as evidence in the course of prosecuting an environmental crime or civil violation will have the same or better evidentiary value as its paper equivalent. Therefore, an electronic report receiving system must establish:

1.That an ER was sent or not sent

2.Date/time document was sent

3.By whom the document was sent; both the individual and entity he/she represents

4.Date/time document was received

5.That the document was not altered from time sent to time received

6.The contents of the document

7.Ability to store and retrieve ER'

regarding time of transmission, receipt and authorship.

Response:
Ohio EPA agrees that all of these are important except the importance of knowing whether an electronic report was not sent (#1 above). Currently the agency receiving systems send reply e-mails to the sender stating whether or not the transmission was accepted. However, for some of our programs, like our Hazardous Waste program, we don't always know which facilities have decided to submit electronically. They may apply for a Personal Identification Number (PIN), but not use it. Also, it is up to the facilities to comply with the regulations when applicable and

Ohio EPA's PIN method does not meet the requirement of #3. In the data table in which the PIN is stored, the PIN is associated with the secondary ID (indicating an organization or facility) and not with the individual who applied for it on a paper form.

P. 46191, Subpart D, section 3.2000 (d)
Submitter Registration Process
US EPA PROPOSES THAT ANYONE WHO SUBMITS ELECTRONIC DOCUMENTS BE REQUIRED

DOCUMENTS TO BE SUBMITTED. THE PERSON WHO IS NOT BEING ISSUED AN ELECTRONIC SIGNATURE WILL SIMPLY NOT BE REQUIRED TO ADHERE TO THE SIGNATURE-SPECIFIC REQUIREMENTS OF THE REGISTRATION PROCESS OF THE REGISTRATION PROCESS. SHOULD THIS MORE GENERAL REGISTRATION REQUIREMENT BE ESTABLISHED?

Response:
Although not specifically defined, the rule requires that "the registration process would also be required to establish the identity of the registering individual and any entity that the individual is authorized to represent". Assumption is that the individual wishing to send data electronically would have to provide identification and, at a minimum, have the signed certification statement notarized and submitted for processing. Is this assumption correct? If not, how does EPA intend to implement this requirement so as not to be burdensome to the regulated users.

SHOULD BE MAINTAINED IN PAPER. CROMERRR PROPOSES AN AGREEMENT BE SIGNED BY THE DIGITAL SIGNATORY DURING REGISTRATION AND UPON SURRENDER OF THE ELECTRONIC SIGNATURE THAT ASSURES HE/SHE:

1.Has protected the signature from use by others.
2.Is legally bound by electronic signature.
3.Cannot delegate use of electronic signature.
4.Affirms that he or she received a copy of the submission which they submitted.
5.Attest to reviewing the copy as well as acknowledgment of submission.
6. Under obligation and followed through with reporting any suspected compromise of signature within 24 hours of discovery.
7. Report within 24 hours any discrepancy between what was signed and submitted and what was acknowledged as received.
8.Attests to complying with terms of signature registration agreement.
9. Has reviewed, signed, submitted all electronic documents submitted with his/her electronic signature.

Response:

Yes, the original certificate/registration assignment should be maintained on paper, so as to have visual access to the person's handwritten signature. It may be needed as verification in an enforcement proceeding. Ref #3 above on delegation of use of the electronic signature. This should allow flexibility to accommodate state-specific regulations. Ohio Administrative Code Rule 3745-50-42 requires that all reports shall be signed by one of the following: a responsible corporate officer; a general partner or the proprietor; for public agencies, a principal executive officer or ranking elected official; or a duly authorized representative of any of these three persons. A limited amount of delegation is allowed based on specific criteria. The certifier frequently is not the preparer. A distinction between them should be allowed and acknowledged. (For the TRI CDX program both the preparer and certifier register.) Ref #'s 6-7 (3.2000 (d) (3) (v) above, it would be more realistic to state that the discovery should be reported by the end of the next business day. What if the discovery is made late on a Friday?

Submitter "Exit" Certification

Response:

With all the previous requirements for registration, re-registration, having the signatures "bound" to the electronic documents, etc, this requirement seems redundant and burdensome.

P. 46191, Subpart D, Section 3.2000 (d)

General Registration for Submitters

US EPA proposes that anyone who submits electronic documents be required to register whether or not they require an electronic signature for the documents to be submitted. The person who is not being issued an electronic signature will simply not be required to adhere to the signature-specific requirements of the registration process.

Response: General registration by the sender does not appear to be necessary for data which doesn't require a certification. The sender is usually identified in some manner within the data or by the transmission mechanism, and most certainly it would contain the facility identification. The organization that operates the facility is required to provide accurate and complete information and we would view the submission the same as if it were on paper.

Although not specifically defined, the rule requires that "the registration process would also be required to establish the identity of the registering individual and any entity that the individual is authorized to represent". Assumption is that the individual wishing to send data electronically would have to provide identification and, at a minimum, have the signed certification statement notarized and submitted for processing. Is this assumption correct? If not, how does EPA intend to implement this requirement so as not to be burdensome to the regulated users.

SHOULD BE MAINTAINED IN PAPER.

Response:

Yes, the original certificate/registration assignment should be maintained on paper, so as to have visual access to the person's handwritten signature. It may be needed as verification in an enforcement proceeding. Ref #3 above on delegation of use of the electronic signature. This should allow flexibility to accommodate state-specific regulations. Ohio Administrative Code Rule 3745-50-42 requires that all reports shall be signed by one of the following: a responsible corporate officer; a general partner or the proprietor; for public agencies, a principal executive

officer or ranking elected official; or a duly authorized representative of any of these three persons. A limited amount of delegation is allowed based on specific criteria. The certifier frequently is not the preparer. A distinction between them should be allowed and acknowledged. (For the TRI CDX program both the preparer and certifier register.) Ref #'s 6-7 (3.2000 (d) (3) (v) above, it would be more realistic to state that the discovery should be reported by the end of the next business day. What if the discovery is made late on a Friday?

Ref **(e)**:

(e) Electronic signature/certification scenario. An acceptable electronic document receiving system that may be used to accept electronic documents bearing an electronic signature must

(1) Not allow an electronic signature to be affixed to the electronic document until:

(i) The signatory has been provided an opportunity to review all of the data to be transmitted in an on-screen visual format that clearly associates the descriptions or labeling of the information being requested with the signatory's response and which format is identical or nearly identical to the visual format in which a corresponding paper document would be submitted; and

(ii) A certification statement that is identical to that which would be required for a paper submission of the document appears on-screen in an easily-read format immediately above a prompt to affix the certifying signature, together with a prominently displayed warning that by affixing the signature the signatory is agreeing that he or she is the authorized signature holder--referred to by name--has protected the security of the signature as required by the electronic signature agreement signed under paragraph (d)(3) of this section and is otherwise using the signature in compliance with the electronic signature agreement;

Response: Part (i) is necessary. The first part of (ii) on the identical certification statement is reasonable, but the second part of (ii), the warning, appears to be unnecessary because the signatory has already signed an electronic signature agreement. Furthermore, it is inconsistent with "an easily-read format ...."

Ref **(2) (i - ii)**

Response: Post-assent acknowledgment via an out-of-band communication does not add to certainty of the electronic signature or record. Acknowledgment may be necessary under some other legal requirement but it should not be required in this context because acknowledgment does not add to the certainty of a record. However, pre-assent and out-of-band communication of a record does add to the certainty for the signing of a record provided that the purported signatory is given a time period in which to repudiate the signature.

(f) Transaction Record. An acceptable electronic document receiving system must create a transaction record for each received electronic document that includes:

(1) The precise routing of the electronic report from the submitter's computer to the electronic document receiving system;

Response: This seems excessive. Wouldn't proof that the transmission was encrypted from end to end be enough?

(i) Initial receipt of the electronic document;

(ii) Sending of electronic acknowledgment under paragraph (e)(2) of this section;

(iii) Copy of record created under paragraph (e)(3) of this section;

Response: (2)(i) appears to be the only item needed. Acknowledgment should not always be needed (see comment to (e)(2)). Keeping date and time of acknowledgments is excessive in many cases. Likewise, maintaining date and time of the copy of record does not appear to reasonably add assurance to the electronic record.

p. 46192, Subpart D, section 3.2000, (e) (3)
Criteria for Acceptable Electronic Document Receiving Systems

A "Copy of Record" is proposed where exact duplicate of record submitted is sent back to submitter as a method of enabling timely disavowal of unintended submission and reducing the frequency and claims that an ER has been modified in transmission or unintentionally submitted.

Response:

Yes, however, chain-of-custody requirements for electronic submittals are more restrictive and burdensome that those currently required by hard copy submissions. Ohio does not currently track (nor do we believe any other state tracks) the "chain-of-custody" of paper submissions for Discharge Monitoring Reports. It is difficult to confirm chain-of-custody requirements for paper submissions from regulated entities and even more difficult with an electronic reporting system.

P. 46192, Subpart D, section 3.2000, (f) (1)
Precise Routing Information for the Submission.

Response:

This is not possible given our current electronic reporting systems. The precise routing of e-mail submissions and collecting packet header information is not typically done. This information is stripped off and not included with the electronic information.

P.46192, Subpart D, section 3.2000 (f) (3)

Keeping a copy of record as part of the "transaction record" seems redundant in that (e)(3) already requires that the copy of record be created and archived.

Ref **(g) (ii)**

Response: This requirement appears more rigorous than paper. The capture of the display would be appropriate (mimicking paper), but capturing the sequence may be excessive. On one hand, sequence can be compared to page numbers, but on the other hand, when multiple documents are signed manually, the sequence is not necessarily intrinsic to the signature process nor recorded in and of itself.

REQUIREMENTS SUFFICIENT TAKEN TOGETHER TO PROTECT THE AUTHENTICITY AND INTEGRITY OF THE RECORDS RECEIVED AND MAINTAINED?

Receiving systems must have:

- Robust protections against unauthorized access
- Protections against unauthorized use of any electronic signature
- Provide for detection of unauthorized access or attempted access to the system or electronic signature

- Provide safeguards preventing modification of document
- Ensure every electronic record is protected from modification or deletion
- Provide safeguards to ensure that system clock is accurate and protected from tampering or any compromise
- Safeguards for prevention of any corruption or compromise of the system

Response:
Regarding unauthorized access safeguards, and the requirement for a state to show "robust protection" What is US EPA's yardstick for determining if a system is okay to be a receiving system? If a state operates a firewall and uses password protection, would this be considered " robust protection"?

p.46192, Subpart D, section 3.2000, (e) (1) (i), (ii)
Criteria for acceptable electronic document receiving systems
Electronic Document Receiving Systems must validate only electronic signatures affixed after:

1. Submitter has scrolled through on-screen pages in human-readable format.
2. Screen displays a certification statement that is similar or identical to certifying language required on paper submissions.
3. Includes a warning that by signing the submitter agrees that he or she is using the signature in compliance with the agreement that was signed when the signature device was issued.

US EPA ASKS FOR COMMENTS; ESPECIALLY INTERESTED IN THE QUESTIONS OF WHETHER ANY OF THESE PROVISIONS MIGHT TEND TO DISCOURAGE REGULATED ENTITIES FROM CHOOSING TO SUBMIT ENVIRONMENTAL REPORTS ELECTRONICALLY.

Response:
Requirement #1 to scroll through on-screen pages prior to signing is unnecessary and redundant. The individual responsible for signing documents, electronic or otherwise, would already be aware of his legal obligations. Additionally, for electronic submission, he has already "signed" for and certified that he understands his responsibilities in using the electronic signature.

P.46192, Subpart D, section (e) (2) (ii)
Electronic signature/certification
US EPA IS SEEKING COMMENT ON PREVENTING UNAUTHORIZED USE OF AN ELECTRONIC SIGNATURE BY SENDING THE AUTOMATIC ACKNOWLEDGMENT TO AN ADDRESS THAT DOES NOT SHARE THE SAME ACCESS CONTROL (NOT PROTECTED BY THE SAME PASSWORDS OR LOG-IN PROCEDURES AS THE SYSTEM FROM WHICH THE ER WAS SIGNED AND SENT).

Response:
Return receipt (acknowledgment) requirements may be overkill. In the paper-based environment, this does not necessarily happen as part of the legality of a document. Why does the acknowledgment have to go to some place access-controlled?

P. 46192, Subpart D, Sec. 3.3000
How are authorized State, tribal or local environmental programs modified to allow electronic record-keeping?
Response:

Despite the U.S. EPA's comments that there is no impact on state agencies because they have a choice in using electronic reporting and record-keeping under the rule, there is an impact on a state agency that currently accepts electronic reporting under a U.S. EPA program. In that instance, the state agency must either bear the financial impact of returning to a paper-based transaction system or revising/modifying its electronic system to conform to CROMERRR. In either case, there is a financial impact.

123:3-1-01 USE OF ELECTRONIC SIGNATURES AND RECORDS.

(A) DEFINITIONS. IN ADDITION TO THE DEFINITIONS IN SECTION 1306.01 OF THE REVISED CODE, THE FOLLOWING DEFINITIONS ARE ALSO APPLICABLE TO THIS RULE:

(1) "AUTHENTICATION" IS THE ASSURANCE THAT THE ELECTRONIC SIGNATURE IS THAT OF THE PERSON PURPORTING TO SIGN A RECORD OR OTHERWISE CONDUCTING AN ELECTRONIC TRANSACTION.

(2) "DOMAIN" MEANS CATEGORY OF PERSONS BASED ON THE NATURE OF THE IDENTITY OF THE PERSON.

(3) "ELECTRONIC TRANSACTION" MEANS THE EXCHANGE OF AN ELECTRONIC RECORD AND/OR ELECTRONIC SIGNATURE BY A STATE AGENCY WITH A PERSON TO:

(a) FACILITATE ACCESS TO RESTRICTED INFORMATION;
(b) PURCHASE, SELL OR LEASE GOODS, SERVICES OR CONSTRUCTION;
(c) TRANSFER FUNDS;
(d) FACILITATE THE SUBMISSION OF AN ELECTRONIC RECORD OR ELECTRONIC SIGNATURE REQUIRED OR ACCEPTED BY A STATE AGENCY; OR
(e) CREATE RECORDS UPON WHICH THE STATE OF OHIO OR AN OTHER PERSON WILL REASONABLY RELY INCLUDING BUT NOT LIMITED TO FORMAL COMMUNICATION, LETTERS, NOTICES, DIRECTIVES, POLICIES, GUIDELINES AND ANY OTHER RECORD THAT IS FORMALLY ISSUED UNDER A SIGNATURE. THIS SUBSECTION DOES NOT INCLUDE INFORMATIONAL PUBLICATIONS AND INFORMAL COMMUNICATIONS.

(4) "INTEGRITY" IS THE ASSURANCE THAT THE ELECTRONIC RECORD IS NOT MODIFIED FROM WHAT THE SIGNOR ADOPTED.

(5) "NONREPUDIATION" IS THE PROOF THAT THE SIGNOR ADOPTED OR ASSENTED TO THE ELECTRONIC RECORD OR TRANSACTION.

(B) GENERAL RULE.

(1) ELECTRONIC TRANSACTIONS HAVE THE EQUIVALENT LEVEL OF LEGAL PROTECTION THAT IS GIVEN TO PAPER-BASED

TRANSACTIONS. ALL SECURITY PROCEDURES AND TECHNOLOGIES SHOULD PROVIDE AUTHENTICATION, NONREPUDIATION AND INTEGRITY TO THE EXTENT THAT IS REASONABLE FOR EACH ELECTRONIC TRANSACTION.

(2) THIS RULE ESTABLISHES AN OVERARCHING SECURITY PROCEDURE THAT REQUIRES STATE AGENCIES TO:

(a) REPORT ELECTRONIC TRANSACTIONS TO THE DEPARTMENT OF ADMINISTRATIVE SERVICES (DAS);
(b) CONDUCT A SECURITY ASSESSMENT OF EACH SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS;
(c) USE MINIMUM TECHNOLOGY STANDARDS AND/OR SECURITY PROCEDURES THAT ARE APPROPRIATE FOR THE LEVEL OF SECURITY AS DETERMINED BY THE SECURITY ASSESSMENT;
(d) OBTAIN DAS APPROVAL THAT THE SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS CONFORMS TO THE MINIMUM TECHNOLOGY STANDARDS FOR EACH LEVEL OF SECURITY IDENTIFIED IN THE SECURITY ASSESSMENT OR SEEK A WAIVER; AND
(e) ESTABLISH AND MAINTAIN DOCUMENTED SECURITY POLICIES AND PROCEDURES.

(C) SCOPE.

(1) THIS RULE ONLY APPLIES TO ELECTRONIC TRANSACTIONS TO:

(a) FACILITATE ACCESS TO RESTRICTED INFORMATION;
(b) PURCHASE, SELL OR LEASE GOODS, SERVICES OR CONSTRUCTION;
(c) TRANSFER FUNDS;
(d) FACILITATE THE SUBMISSION OF AN ELECTRONIC RECORD OR ELECTRONIC SIGNATURE REQUIRED OR ACCEPTED BY A STATE AGENCY; OR
(e) CREATE RECORDS UPON WHICH THE STATE OF OHIO OR AN OTHER PERSON WILL REASONABLY RELY INCLUDING BUT NOT LIMITED TO FORMAL COMMUNICATION, LETTERS, NOTICES, DIRECTIVES, POLICIES, GUIDELINES AND ANY OTHER RECORD THAT IS FORMALLY ISSUED UNDER A SIGNATURE. THIS SUBSECTION DOES NOT INCLUDE INFORMATIONAL PUBLICATIONS AND INFORMAL COMMUNICATIONS.

(2) THIS RULE APPLIES ONLY TO ELECTRONIC TRANSACTIONS INVOLVING A STATE AGENCY.

(D) REPORTING USES OF ELECTRONIC TRANSACTIONS.

(1) FOR EACH SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS, STATE AGENCIES MUST PROVIDE AN ELECTRONIC TRANSACTION REPORT TO DAS AND REQUEST DAS APPROVAL OF COMPLIANCE WITH THIS RULE OR A WAIVER OF THIS RULE. A STATE AGENCY MUST SUBMIT THE REPORT AND HAVE RECEIVED APPROVAL OR WAIVER OF THE REQUEST BEFORE ACQUIRING OR IMPLEMENTING ELECTRONIC SIGNATURES, TRANSACTIONS OR RELATED TECHNOLOGY.

(2) THE APPROVAL REQUEST IS A LETTER TO DAS IDENTIFYING THE SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS AND STATING THAT THE STATE AGENCY IS SEEKING APPROVAL. THE REQUEST ALSO INCLUDES THE ELECTRONIC TRANSACTION REPORT.

(3) THE WAIVER REQUEST IS A LETTER TO DAS IDENTIFYING THE ELECTRONIC TRANSACTION SET, STATING THE STATE AGENCY IS SEEKING A WAIVER AND PROVIDING A JUSTIFICATION FOR THE WAIVER. THE REQUEST FOR WAIVER ALSO INCLUDES THE ELECTRONIC TRANSACTION REPORT. THE JUSTIFICATION MUST SHOW THAT THE PROPOSED ALTERNATIVE SECURITY TECHNOLOGY OR PROCEDURES PROVIDE AUTHENTICATION, NONREPUDIATION AND INTEGRITY AND DO NOT COMPROMISE THE LEVEL OF SECURITY AS DETERMINED BY PARAGRAPHS (F) AND (G) OF THIS RULE.

(4) EACH ELECTRONIC TRANSACTION REPORT MUST INCLUDE:

(a) THE IDENTIFICATION AND DESCRIPTION OF THE SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS;
(b) THE DOMAIN UNDER WHICH THE ELECTRONIC TRANSACTION SET FALLS;
(c) A SECURITY ASSESSMENT THAT IDENTIFIES THE POTENTIAL IMPACT OF A SECURITY BREACH AND THE RISK OF SUCH A BREACH OCCURRING;

(d) A DETERMINATION OF THE SECURITY LEVEL REQUIRED FOR THE ELECTRONIC TRANSACTION SET PER THE SECURITY ASSESSMENT;
(e) THE SECURITY PROCEDURE USED FOR THE ELECTRONIC TRANSACTION SET; AND
(f) A LIST OF DOCUMENTED AGENCY SECURITY POLICIES FOR PHYSICAL, NETWORK AND COMPUTER SECURITY. THESE DOCUMENTS MUST BE CLEARLY REFERENCED AND MAINTAINED ON FILE AND AVAILABLE FOR AUDIT.

(5) STATE AGENCIES MUST SUBMIT THE REPORT AS EARLY IN THE PROCESS AS POSSIBLE. AGENCIES MUST UPDATE EACH REPORT QUARTERLY. IF DAS DETERMINES THAT AN UPDATE CONSTITUTES A SUBSTANTIAL MODIFICATION OR A NEW ELECTRONIC TRANSACTION, DAS MAY REQUIRE THAT THE STATE AGENCY SUBMIT A NEW REQUEST FOR APPROVAL OR A WAIVER.

(6) WHILE STATE AGENCIES MAY CONTINUE TO USE ELECTRONIC TRANSACTIONS THAT WERE AUTHORIZED BY LAW, ADMINISTRATIVE RULE OR POLICY PRIOR TO SEPTEMBER 13, 2000 FOR TWO YEARS PURSUANT TO SECTION 1306.20 OF THE REVISED CODE, AGENCIES CONTINUING TO USE PRIOR ELECTRONIC TRANSACTIONS MUST FILE AN ELECTRONIC TRANSACTION REPORT WITH DAS WITHIN THREE MONTHS OF THE EFFECTIVE DATE OF THIS RULE ALTHOUGH THE ELECTRONIC TRANSACTIONS NEED NOT CONFORM WITH THE THIS RULE OR HAVE DAS APPROVAL.

(E) ELECTRONIC TRANSACTION DOMAINS. PERSONS USING ELECTRONIC TRANSACTIONS IN THE COURSE OF GOVERNMENT AFFAIRS FALL IN ONE OF THREE DOMAINS – THE CITIZEN DOMAIN, THE BUSINESS DOMAIN OR THE STATE INTERNAL DOMAIN.

(1) CITIZEN DOMAIN: THE CITIZEN DOMAIN CONSISTS OF INDIVIDUALS ACTING ON THEIR OWN BEHALF OR ON THE BEHALF OF AN ANOTHER INDIVIDUAL UNDER A POWER OF ATTORNEY. THE CITIZEN DOMAIN INCLUDES ONLY THOSE INDIVIDUALS WHO CHOOSE TO INTERACT ELECTRONICALLY WITH THE STATE OF OHIO. THE CITIZEN DOMAIN ALSO INCLUDES STATE WEB AND APPLICATION SERVERS THAT INTERACT WITH CITIZENS.

(2) BUSINESS DOMAIN: THE BUSINESS DOMAIN CONSISTS OF CORPORATIONS, BUSINESS TRUSTS, PARTNERSHIPS, LIMITED LIABILITY COMPANIES, ASSOCIATIONS, JOINT VENTURES OR ANY OTHER COMMERCIAL, CHARITABLE OR LEGAL ENTITY THAT INTERACTS ELECTRONICALLY WITH STATE AGENCIES. THIS DOMAIN ALSO INCLUDES WEB AND APPLICATION SERVERS THAT INTERACT WITH BUSINESSES.

(3) STATE INTERNAL DOMAIN: THE STATE INTERNAL DOMAIN CONSISTS OF STATE EMPLOYEES ACTING ON BEHALF OF THE STATE, AND ANY OTHER AGENT OF THE STATE; NETWORK COMPONENTS; AND WEB AND APPLICATION SERVERS THAT USE ELECTRONIC TRANSACTION-ENABLED APPLICATIONS FOR THE CONDUCT OF INTERNAL STATE BUSINESS. THE STATE INTERNAL DOMAIN ALSO APPLIES TO LOCAL GOVERNMENT REPRESENTATIVES FOR ELECTRONIC TRANSACTIONS WITH STATE GOVERNMENT AGENCIES.

(F) SECURITY ASSESSMENT.

(1) IN ORDER TO RECEIVE APPROVAL FROM DAS, AGENCIES MUST COMPLETE A SECURITY ASSESSMENT FOR THE USE OF THE SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS. THE SECURITY ASSESSMENT IDENTIFIES THE APPROPRIATE SECURITY LEVEL BY ANALYZING THE IMPACT OF A SECURITY BREACH AND THE RISK OF A SECURITY BREACH.

(2) IN DETERMINING THE POTENTIAL IMPACT OF A SECURITY BREACH, STATE AGENCIES WILL CONSIDER THE:

(a) INTENDED USE OF THE ELECTRONIC RECORD OR SIGNATURE;
(b) TYPE OF INFORMATION BEING TRANSMITTED, RECEIVED OR STORED;
(c) NETWORK USED;
(d) DEGREE OF RISK TO THE STATE;
(e) DEGREE OF RISK TO THE USERS OF THE SYSTEM;
(f) DEGREE OF RISK TO THIRD PARTIES;
(g) PROJECTED VOLUME OF TRANSACTIONS;
(h) EFFECTIVENESS OF THE SECURITY PROCEDURES;
(i) ESTIMATED COST;
(j) POTENTIAL LEGAL LIABILITY; AND

(k) APPROPRIATE REQUIREMENTS FOR AUTHENTICATION OF IDENTITY.

(3) IMPACT OF A SECURITY BREACH. THE POTENTIAL IMPACT OF A SECURITY BREACH FALLS IN ONE OF FOUR CATEGORIES – LOW-IMPACT, MEDIUM-IMPACT, HIGH-IMPACT AND VERY HIGH-IMPACT.

(a) LOW-IMPACT: A SECURITY BREACH IS CONSIDERED LOW-IMPACT IF THERE IS NO IMPACT OF A BREACH OF SECURITY OR THE IMPACT IS DE MINIMIS OR SO INSIGNIFICANT THAT THERE WOULD BE NO OR ONLY A DE MINIMIS FINANCIAL LOSS, LOSS OF THE PUBLIC'S TRUST OR LEGAL CONSEQUENCES.

(b) MEDIUM-IMPACT: A SECURITY BREACH IS CONSIDERED MEDIUM-IMPACT IF THE IMPACT IS LIMITED IN NATURE. LIMITED IN NATURE MEANS THAT THE FINANCIAL LOSS WHEN AVERAGED FOR THE ELECTRONIC TRANSACTION SET IS LESS THAN TEN THOUSAND DOLLARS TO THE BUSINESS, CITIZEN, STATE OR OTHER ENTITY INVOLVED, THAT THERE ARE NO MAJOR LEGAL IMPLICATIONS AND THAT THE BREACH WOULD NOT CAUSE SIGNIFICANT PUBLIC DISTRUST FOR THE STATE.

(c) HIGH-IMPACT: A SECURITY BREACH IS CONSIDERED HIGH-IMPACT IF THE COMPROMISED SECURITY WOULD HAVE A SIGNIFICANT IMPACT. THE FINANCIAL HARM WHEN AVERAGED FOR THE ELECTRONIC TRANSACTION SET RANGES FROM TEN THOUSAND DOLLARS TO FIVE HUNDRED THOUSAND DOLLARS. THE BREACH WOULD RESULT IN MEDIA SCRUTINY AND SIGNIFICANT PUBLIC DISTRUST OR WOULD BE FOLLOWED BY LEGAL CONSEQUENCES.

(d) VERY HIGH-IMPACT: THE RESULT OF A SECURITY BREACH THAT HAS A VERY HIGH IMPACT WOULD BE EXTREMELY SERIOUS. IN THE EVENT OF THIS TYPE OF BREACH, THE FINANCIAL CONSEQUENCES WHEN AVERAGED FOR THE ELECTRONIC TRANSACTION SET WOULD EXCEED FIVE HUNDRED THOUSAND DOLLARS OR RESULT IN CONSIDERABLE LEGAL VIOLATIONS OR

CAUSE INTENSE MEDIA SCRUTINY AND WIDESPREAD, DEEP PUBLIC DISTRUST.

(4) RISK OF A SECURITY BREACH. THE RISK OF A BREACH IS A DETERMINATION OF THE LIKELIHOOD OF SOMEONE TRYING TO BREACH THE SECURITY FOR THE SPECIFIC ELECTRONIC TRANSACTION. THE PRIMARY CONSIDERATION IS THE VALUE OF A SECURITY BREACH TO A PERSON ATTEMPTING A BREACH. VALUE INCLUDES FINANCIAL GAIN, UNAUTHORIZED ACCESS TO CONFIDENTIAL INFORMATION AND THE ABILITY TO HARASS, EMBARRASS OR SHOCK. THE RISK IS CHARACTERIZED AS LOW, MEDIUM OR HIGH.

(a) LOW-RISK: A LOW-RISK ELECTRONIC TRANSACTION IS ONE THAT WOULD HAVE LITTLE VALUE TO SOMEONE ATTEMPTING A BREACH, AND THEREFORE, THE LIKELIHOOD OF BREACH ATTEMPTS IS SMALL WITH ANY ATTEMPTS LIKELY TO BE NONE OR FEW AND LIMITED IN EFFORT.

(b) MEDIUM-RISK: A MEDIUM-RISK ELECTRONIC TRANSACTION IS ONE WHICH WOULD PROVIDE VALUE TO SOMEONE SEEKING TO BREACH SECURITY.

(c) HIGH-RISK: A HIGH-RISK ELECTRONIC TRANSACTION WOULD PROVIDE GREAT VALUE TO SOMEONE SHOULD HE OR SHE BREACH SECURITY.

(5) SECURITY ASSESSMENT. THE SECURITY ASSESSMENT RESULTS IN A DETERMINATION THAT THE ELECTRONIC TRANSACTION FALLS WITHIN ONE OF FOUR MINIMUM SECURITY LEVELS – LOW (LEVEL A), MEDIUM (LEVEL B), HIGH (LEVEL C) OR VERY HIGH (LEVEL D). THE MINIMUM SECURITY LEVEL IS DETERMINED BY THE COMBINATION OF THE LEVEL OF THE IMPACT OF A SECURITY BREACH AND THE LEVEL OF RISK OF A SECURITY BREACH AS IDENTIFIED IN THE FOLLOWING TABLE:

SECURITY ASSESSMENT AS DETERMINED BY THE IMPACT OF A SECURITY BREACH AND THE RISK OF A SECURITY BREACH

	LOW-RISK	MEDIUM-RISK	HIGH-RISK
LOW-IMPACT	LEVEL A	LEVEL A	LEVEL B
MEDIUM-IMPACT	LEVEL B	LEVEL B	LEVEL B

HIGH-IMPACT	LEVEL B	LEVEL C	LEVEL C
VERY HIGH-IMPACT	LEVEL C	LEVEL C	LEVEL D

(G) SECURITY PROCEDURES APPROPRIATE FOR SECURITY LEVELS. EACH ELECTRONIC TRANSACTION SET MUST CONFORM TO THE MINIMUM SECURITY PROCEDURES INCLUDING TECHNOLOGY STANDARDS FOR EACH LEVEL OF SECURITY IDENTIFIED IN THE SECURITY ASSESSMENT. STATE AGENCIES MAY CHOOSE TO MEET THE REQUIREMENTS OF HIGHER SECURITY LEVELS WITH LEVEL A BEING LEAST SECURE AND LEVEL D BEING THE MOST HIGHLY SECURE.

(1) REGARDLESS OF THE LEVELS OF SECURITY IDENTIFIED IN PARAGRAPHS (G)(2) TO (G)(5) OF THIS RULE, THE TRANSMISSION OF USER-IDS AND PASSWORDS MUST BE ENCRYPTED USING SECURE SOCKETS LAYER OR EQUIVALENT ENCRYPTION WHEN TRANSMITTED OVER THE INTERNET OR OTHER UNSECURED NETWORKS.

(2) LEVEL A: UNDER THIS LEVEL OF SECURITY, STATE AGENCIES MAY USE ANY TECHNOLOGICAL MEANS FOR THESE SETS OF ELECTRONIC TRANSACTIONS. THESE ELECTRONIC TRANSACTIONS REQUIRE LITTLE TO NO SECURITY. STATE AGENCIES SHOULD NOTE THAT ELECTRONIC TRANSACTIONS THAT FALL UNDER LEVEL A ARE ONLY THOSE THAT DO NOT INVOLVE A LEGALLY BINDING RECORD, A SIGNATURE, A FINANCIAL TRANSACTION OR CONFIDENTIAL INFORMATION.

(3) LEVEL B: LEVEL B REQUIRES AT A MINIMUM THE USE OF A UNIQUE USER-ID AND A RANDOMLY ASSIGNED ALPHANUMERIC PERSONAL IDENTIFICATION NUMBER CONSISTING OF AT LEAST EIGHT CHARACTERS OR A SMARTCARD OR PHYSICAL DEVICE WITH A UNIQUE PROPRIETARY RANDOM PERSONAL IDENTIFICATION NUMBER AS AN ALTERNATIVE. STATE AGENCIES SEEKING APPROVAL OF LEVEL B ELECTRONIC TRANSACTION SETS MUST PROVIDE A DESCRIPTION OF THE AUTHENTICATION PROCESS INCLUDING INFORMATION ON THE INITIAL REGISTRATION PROCESS AND THE MEANS USED TO PROVE THE IDENTITY OF PERSONS REGISTERING TO USE ELECTRONIC TRANSACTIONS.

(4) LEVEL C: UNDER LEVEL C SECURITY, STATE AGENCIES MUST USE DIGITAL CERTIFICATES PURSUANT TO PARAGRAPH (G)(4)(A) OF THIS RULE FOR THESE ELECTRONIC TRANSACTION SETS OR THE ALTERNATIVE IN PARAGRAPH (G)(4)(b) OF THIS RULE.

(a) DIGITAL CERTIFICATES REQUIRE A SIGNIFICANT INFRASTRUCTURE KNOWN AS PUBLIC KEY INFRASTRUCTURE (PKI). PURSUANT TO SECTION 1306.21 OF THE REVISED CODE, THERE SHALL BE ONE PUBLIC KEY INFRASTRUCTURE FOR STATE AGENCIES, CREATED AND MAINTAINED BY THE DAS.

(i) THE STATE PKI PROVIDES DIGITAL CERTIFICATES FOR PERSONS WITHIN THE STATE INTERNAL DOMAIN, THE BUSINESS DOMAIN AND THE CITIZEN DOMAIN FOR INTERACTING WITH STATE AGENCIES AND ONLY STATE AGENCIES. THE STATE PUBLIC KEY INFRASTRUCTURE SHALL ALSO BE AVAILABLE FOR USE BY THE GENERAL ASSEMBLY, ANY LEGISLATIVE AGENCY, THE SUPREME COURT, THE OTHER COURTS OF RECORD IN THIS STATE OR ANY JUDICIAL AGENCY.

(ii) IN ESTABLISHING THE PKI, DAS HAS SOLE RESPONSIBILITY FOR THE REGISTRATION PROCESS AND AUTHORITIES; CERTIFICATE POLICIES AND CERTIFICATE PRACTICES STATEMENTS, CERTIFICATE MANAGEMENT INCLUDING ISSUANCE, CONTINUED PARTICIPATION, CERTIFICATE REVOCATION AND CERTIFICATE SUSPENSION; AND ANY OTHER PKI POLICY, PRACTICE, MANAGEMENT OR OPERATION. DAS MAY DELEGATE ANY OR ALL COMPONENTS OF THE PKI TO STATE AGENCIES OR TO VENDORS. DAS MAY REVOKE DELEGATION OF PKI COMPONENTS TO A STATE AGENCY OR A VENDOR IN THE EVENT THAT THE STATE AGENCY OR VENDOR IS IN NONCOMPLIANCE WITH THIS RULE, A CERTIFICATE POLICY OR ANY OTHER PKI POLICY.

(iii) DAS OR ITS DELEGATEE MAY REVOKE THE DIGITAL CERTIFICATE OF ANY PERSON WHOSE USE OF THE DIGITAL CERTIFICATE IS NOT IN CONFORMANCE WITH THIS RULE, A CERTIFICATE POLICY OR ANY OTHER PKI POLICY.

(b) AS AN ALTERNATIVE, AGENCIES MAY MEET LEVEL C SECURITY BY COMBINING THE USE OF A UNIQUE USER-ID AND A RANDOMLY ASSIGNED ALPHANUMERIC PERSONAL IDENTIFICATION NUMBER CONSISTING OF AT LEAST EIGHT CHARACTERS WITH A SMARTCARD OR PHYSICAL DEVICE. STATE AGENCIES SEEKING APPROVAL OF ELECTRONIC TRANSACTION SETS USING THIS ALTERNATIVE MUST PROVIDE A DESCRIPTION OF THE AUTHENTICATION PROCESS INCLUDING INFORMATION ON THE INITIAL REGISTRATION PROCESS AND THE MEANS USED TO PROVE THE IDENTITY OF PERSONS REGISTERING TO USE ELECTRONIC TRANSACTIONS. PURSUANT TO SECTION 1306.21 OF THE REVISED CODE, DAS MAY REQUIRE THAT STATE AGENCIES USE A COMMON MULTI-AGENCY SMARTCARD OR PHYSICAL DEVICE INFRASTRUCTURE.

(5) LEVEL D: LEVEL D REQUIRES THE USE OF A DIGITAL CERTIFICATE ISSUED BY DAS COMPUTER SERVICES IN COMBINATION WITH A UNIQUE USER-ID AND A RANDOMLY ASSIGNED ALPHANUMERIC PERSONAL IDENTIFICATION NUMBER CONSISTING OF AT LEAST EIGHT CHARACTERS AND A SMARTCARD OR PHYSICAL DEVICE OR BIOMETRIC. LIKE LEVEL C SECURITY, DAS MAY REQUIRE STATE AGENCIES USE A COMMON MULTI-AGENCY INFRASTRUCTURE. ANY STATE AGENCY USE OF A BIOMETRIC MUST BE IN CONFORMITY WITH DAS POLICIES AND STANDARDS FOR SECURITY, INTEROPERABILITY AND NEED. WHILE STATE AGENCIES MAY USE HIGHER LEVELS OF SECURITY THAN REQUIRED BY THE SECURITY ASSESSMENT, FOR BIOMETRICS, A STATE AGENCY SEEKING TO IMPLEMENT THE USE OF BIOMETRICS MUST PROVIDE A JUSTIFICATION TO DAS.

(H) REQUIRED POLICIES. STATE AGENCIES MUST ESTABLISH DOCUMENTED POLICIES AND PROCEDURES THAT PROVIDE REASONABLE ASSURANCE OF AUTHENTICITY OF SIGNATURES, THE NONREPUDIATION OF THE RECORDS BY THE SIGNATORIES AND THE

INTEGRITY OF THE SIGNED RECORDS. THIS INCLUDES BUT IS NOT LIMITED TO POLICIES AND PROCEDURES ON ACCESS, CONTROL, MONITORING, MAINTENANCE AND ANY OTHER ACTIONS NECESSARY FOR PHYSICAL, NETWORK AND COMPUTER SECURITY. NOTHING IN THIS RULE PERMITS STATE AGENCIES TO SUPERSEDE OR ESTABLISH SECURITY POLICIES IN CONFLICT WITH ANY OTHER POLICY ESTABLISHED BY DAS.

(I) INTERFACE REQUIREMENTS. AT ANY TIME WHEN A STATE AGENCY REQUIRES A SIGNATURE OR IS CONDUCTING A FINANCIAL TRANSACTION, THE STATE AGENCY MUST REQUIRE A SEPARATE AND DISTINCT ACTION ON THE PART OF THE PERSON CONDUCTING THE TRANSACTION FOR FINANCIAL TRANSACTIONS AND EACH SIGNATURE. THE SEPARATE AND DISTINCT TRANSACTION MAY INCLUDE A SERIES OF KEYSTROKES, A CLICK OF MOUSE OR OTHER SIMILAR ACTION. THE SEPARATE AND DISTINCT ACTION MUST ALSO BE CLEARLY MARKED AS INDICATING AN INTENT TO COMPLETE A FINANCIAL TRANSACTION OR TO SIGN A WRITING.

(J) RECORDS RETENTION REQUIREMENTS. STATE AGENCIES' RECORDS RETENTION PRACTICES MUST ASSURE NONREPUDIATION, INTEGRITY AND CONTINUED ACCESS TO THE ELECTRONIC RECORD.

(K) WAIVER PROVISIONS. UPON A STATE AGENCY REQUEST FOR A WAIVER PURSUANT TO PARAGRAPH (D) OF THIS RULE, THE DIRECTOR OF THE DAS OR HIS DESIGNEE MAY WAIVE THE REQUIREMENTS OF THIS RULE FOR AN ELECTRONIC TRANSACTION SET UPON A SHOWING BY THE STATE AGENCY THAT THE ALTERNATIVE SECURITY PROCEDURES GOVERNING THE SET OF PROPOSED SIMILAR ELECTRONIC TRANSACTIONS DO NOT COMPROMISE THE LEVEL OF SECURITY AS DETERMINED BY PARAGRAPHS (F) AND (G) OF THIS RULE.

(L) ELECTRONIC TRANSACTIONS WITH AGENCIES OF OTHER STATES AND THE FEDERAL GOVERNMENT. THIS RULE APPLIES TO ELECTRONIC TRANSACTIONS BETWEEN STATE AGENCIES AND FEDERAL AGENCIES TO THE EXTENT THAT IT IS CONSISTENT WITH FEDERAL LAW. DAS SHALL COORDINATE THE USE OF ELECTRONIC SIGNATURES BETWEEN STATE AGENCIES AND THE FEDERAL GOVERNMENT. DAS SHALL COORDINATE THE USE OF ELECTRONIC SIGNATURES WITH AGENCIES OF ANOTHER STATE.

Effective: December 22, 2000

R.C. 119.032 review dates: December 13, 2005

_____

C. Scott Johnson
Director, Department of Administrative Services

_____

Date

Promulgated under: R.C. 111.15
Statutory authority: R.C. 1306.21
Rule amplifies: R.C. 1306.21